(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 September 2003 (04.09.2003)

PCT

(10) International Publication Number
WO 03/073240 A1

(51) International Patent Classification[7]: G06F 1/00, H04L 9/32

(21) International Application Number: PCT/FI02/00572

(22) International Filing Date: 27 June 2002 (27.06.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20020369 26 February 2002 (26.02.2002) FI

(71) Applicant *(for all designated States except US)*: **COMPTEL CORPORATION** [FI/FI]; Ruoholahdenkatu 4, FIN-00180 Helsinki (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **NARDONE, Massimo** [IT/FI]; Hiomokuja 1 a 24, FIN-00380 Helsinki (FI).

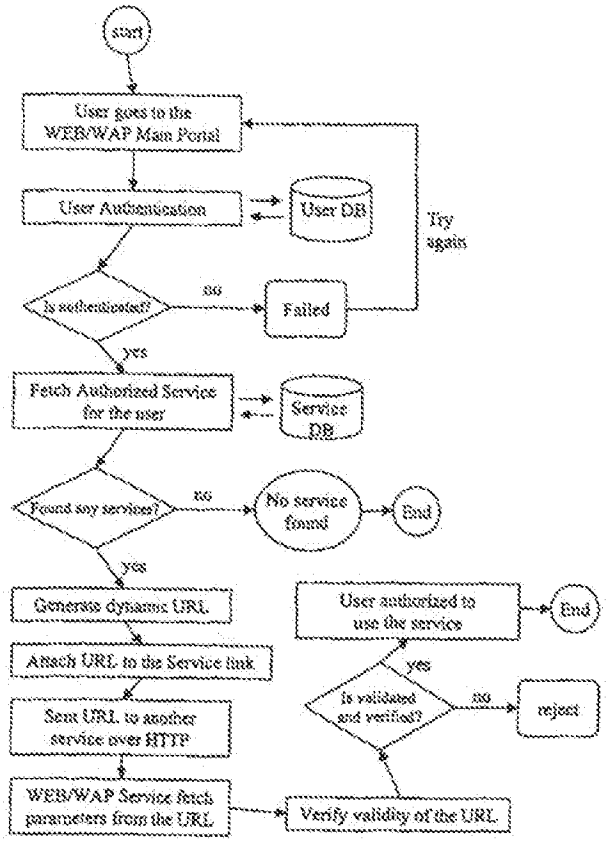
(74) Agent: **SEPPO LAINE OY**; Itämerenkatu 3 B, FIN-00180 Helsinki (FI).

(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: USER AUTHENTICATION BETWEEN RESOURCES IN A DATA NETWORK



(57) Abstract: A method of forwarding user authentication and/or authorization from a first network resource to a second network resource, the method comprising a step of transmitting information verifying the user authentication and/or authorization from a first network resource to a second network resource as a part a dynamic string, such as an URL address pointing to the second network resource. With this aspect of the invention, two or more network resources can share efficiently and securely the user authentication and/or authorization performed at one of the network resources. This inventive concept is particularly suitable for platforms used in electronic commerce (e-commerce) and/or mobile commerce (m-commerce) environments.

WO 03/073240 A1

Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *with international search report*

USER AUTHENTICATION BETWEEN RESOURCES IN A DATA NETWORK

Technical Field

The present invention relates to user authentication in a data network, such as the Internet. More specifically, the present invention relates to transmitting or forwarding a user authentication from a first network resource to a second network resource in such a manner that a user that has been authenticated at the first network resource can be authenticated at the second network resource without the user having to submit separate authentication information to the second network resource. The network resources referred herein include servers and local area networks, for instance.

Background Art

U.S. Patent No. US 6,263,432 discloses a system wherein a computer program memory stores computer instructions for securing data transmitted over the Internet, enabling a user to be authenticated and authorized for a requested operation. An "eticket" architecture (including identification information) is generated by an authentication server. The information in the eticket is hashed using, for example, a Message Digest Protocol, and a hash number is generated. The hash number is then encrypted using a private key, and the identification information in the eticket and the encrypted hash number are concatenated to generate a completed "eticket" architecture. The "eticket" may then be transmitted over the Internet (i.e., a non-secure environment) from server to server without having the information in the "eticket" altered, and without having to "re-authenticate" the user at each server.

User authentication is defined as "determining the true identity of a user or an object attempting to access a system." Any non-public system has to have an authentication system in order to filter and identify users from one another.

User authorization, in turn, involves determining what types of activities are permitted for an authenticated user or object.

The system and method described in US 6,263,432 saves the user from having to "log on" for each new network resource. The system and method also eliminates the need of "authentication" for each "authorization" request made through the network.

Even though it is convenient for the user, the technique presented by US 6,263,432 is cumbersome from the network's point of view.

Disclosure of Invention

In is an object of the present invention to create a system and method wherein a user authentication and/or authorization can be forwarded from a first network resource to a second network resource in a secure but more efficient manner.

The object of the invention is achieved by transmitting the user authentication and/or authorization information as part of a dynamic string transmitted to the second network address. The term dynamic string refers herein to a string of bits that is created for a specific, preferably one-time, use only and is not intended to be maintained or stored for a longer period or for a subsequent use. Thus, a dynamic string is created to exist for a relatively short period of time and intended to vanish or at least be useless and not valid after the expiry of said period of time. The relatively short period of time referred herein may be, depending on the application, for example 1 to 10 and preferably less than 2 minutes.

The dynamic string can be transmitted to the second network resource by any means of data communication. For example, the dynamic string can be an URL (Uniform Resource Locator) address, an SMS (Short Message Service) message or an MMS (Multimedia Messaging Service) message. The dynamic string can also be a message transmitted by means of a socket communication, e.g. TCP/IP (Transmission Control Protocol/Internet protocol), UDP (User Datagram Protocol), SIP (Session Initiation Protocol) or RTP (Real-Time Transport Protocol), for instance.

This inventive concept offers several useful and advantageous aspects and embodiments, which are described in the following.

According to one aspect of the invention, there is provided a method for preparing user authentication and/or authorization information at a first network resource for transmission to a second network resource, the method being performed after authenticating and/or authorizing a user accessing the first network resource and the method comprising a step of preparing a dynamic string. The dynamic string, on its part, comprises at least an address part and a parameter part. The address part contains a

network address (or a corresponding address) that points to the second network resource. The parameter part comprises information verifying the user authentication and/or authorization. With this aspect of the invention, the user authentication and/or authorization information can be sent from the first network resource to the second network resource. The sending of the information may occur, e.g. after the user having selected a link pointing to the second network resource. In an embodiment wherein the dynamic string is a dynamic URL, the sending of the information may occur, e.g. after presenting the prepared dynamic URL as a link on a WEB or WAP page and after the user having activated the link by a mouse click, for instance.

According to another aspect of the invention, there is provided a method for accepting, at a second network resource, a user authentication and/or authorization performed at a first network resource, the method comprising a step of receiving, as a parameter in a dynamic string transmitted to the second network resource, information on the user authentication and/or authorization performed at the first network resource. After receiving the information, the method comprises a step of using a cryptographic method to verify the received user authentication and/or authorization information, and, after the verification, the second network resource accepting the user as an authenticated and/or authorized user for at least one function, service, WEB or WAP page, program, process or any action offered by the second network resource. With this aspect of the invention, the second network resource can authenticate and/or authorize a user coming from another network resource without requesting the user to provide authentication information once again at the second network resource.

According to a further aspect of the invention, there is provided a method of forwarding user authentication and/or authorization from a first network resource to a second network resource, the method comprising a step of transmitting information verifying the user authentication and/or authorization from a first network resource to a second network resource as a part a dynamic string transmitted to the second network resource. With this aspect of the invention, two or more network resources are able to share efficiently and securely the user authentication and/or authorization performed at one of the network resources.

It should be noted that it is also possible to use the present invention for the purposes of the first and second network resources only, i.e. without there being any external users

accessing the first or second network resource. In this case, the transmitted user authentication and/or authorization information relates to the first network resource or an entity within the first network resource. Such an entity may be a program, process or service run at the first network resource.

Considerable benefits are gained with this invention. Primarily, with the invention, there is no need to create, store and transmit an eticket, as in the technique presented in the U.S. Patent No. US 6,263,432 mentioned above. With the invention, no session or cookie is needed to store information about the user. Furthermore, in an advantageous embodiment of the invention, no information at all needs to be stored about the user for a secure authentication and/or authorization at the remote resource. Thus, the invention makes it possible to enhance efficiency in remote authentication and/or authorization.

With the preferred embodiments of the invention, even more advantages can be gained.

In a preferred embodiment in which no additional database or network traffic is needed, the level of security can also be raised as there is practically no traffic for a third party to intervene.

In a preferred embodiment in which no user identification database or a corresponding network resource needs to be contacted by the second network resource, the user making a request at the resource can be authenticated and/or authorized without a delay.

In an embodiment of the invention, the dynamic string contains a hash for checking the integrity of the authentication and/or authorization information in the dynamic string.

In another embodiment, the hash is taken from a data input that contains a secret code known to the first network resource and any second network resource utilizing the method, but unknown to any intervening party. In such an embodiment, it is computationally infeasible to break the dynamic string and form a fake dynamic string containing a correct hash.

In a further embodiment, the dynamic string contains a data sequence varying with time, such as a time stamp, and the hash is taken from an input containing, in addition to the secret code, also the time stamp. In such an embodiment, it is impossible to use even a correct dynamic string if intercepted by a third party because the time stamp in the dynamic string would indicate an expired point of time. The time stamp cannot be

altered either, because it is computationally infeasible to break the dynamic string and form a fake dynamic string containing a correct hash.

In another embodiment, the dynamic string contains a digital signature enabling the second network resource to check the identity of the first network resource.

In another preferred embodiment of the invention wherein the dynamic string is a dynamic URL address, the second network resource reads, from the HTTP Server Variables, the variable titled "REMOTE_ADDR" and picks up the sender's IP address. After getting the IP address, the network resource checks whether the obtained IP address appears on a list of acceptable IP addresses, and if not, denies the user authentication and/or authorization.

As is apparent from the above disclosure, the present invention can be applied in a great variety of applications requiring data communication over a data network, particularly the Internet. The present invention is particularly suitable for platforms used in electronic commerce (e-commerce) and/or mobile commerce (m-commerce) environments. In e-commerce or m-commerce, it is rare that one party controls the whole "portal" of trade or commerce place. Instead, at least some of the services of content will be provided at a server managed by another party. Indeed, it is typical of the process of offering services, content, goods, etc. for there to be at least three parties involved. These parties are an operator, a plurality of service and/or content providers and the users. The operator owns the technical platform, offers accesses for users, collects and stores information about the users (CRM) and manages the actual market or commerce place. The aforesaid activities could be also divided between two or more operators or the like. The service and/or content providers are connected to the aforesaid operator. The users are usually connected to an e- and/or an m-commerce platform via a "portal" or access point (e.g. WEB or WAP), which is maintained by the operator. Furthermore, all of the before said parties can be situated anywhere in the data network.

The present invention can be advantageously applied, e.g. in a dynamic e-commerce or m-commerce system. In an advantageous dynamic e-commerce or m-commerce system, transaction processing and billing of the transactions is implemented so that all parties are able to affect the availability, terms and billing of the transactions. This kind of preferred way to implement dynamic transaction processing is described in Finnish

patent application No. 20012406, which was not published at the time of filing of the present application, and which is incorporated herein by reference.

Finnish patent application No. FI20020699, filed on 11 April 2002 and not published at the time of filing of the present application, describes another particularly interesting portal system in which the present invention could be usefully employed.

Brief Description of Drawings

For a more complete understanding of the present invention and the advantages thereof, the invention is now described with reference to the following drawings, in which:

FIG. 1 depicts an overview of one possible system architecture that can make use of the invention.

FIG. 2 presents a flow diagram of a process according to one embodiment of the invention.

FIG. 3 presents a flow diagram of one process of creating a dynamic URL, according to another embodiment of the invention.

FIG. 4 presents a flow diagram of one process of validating a dynamic URL, according to another embodiment of the invention.

FIG. 5 shows an example of the parameters that can be used in the processes of FIG. 3 and FIG. 4.

FIG. 6 presents a flow diagram of another process of creating a dynamic URL, according to another embodiment of the invention.

FIG. 7 presents a flow diagram of another process of validating a dynamic URL, according to another embodiment of the invention.

FIG. 8 shows an example of the parameters that can be used in the processes of FIG. 6 and FIG. 7.

Best Mode for Carrying Out the Invention

In the following description, the invention is studied by way of examples wherein a dynamic URL address is used as the dynamic string according to the invention. On the basis of this description, it is believed to be apparent to a person skilled in the art how the invention can be utilised with other kinds of dynamic strings, such as strings transmitted by means of socket, UDP, SIP, RTP, SMS or MMS. Thus, the following disclosure is by no way limiting the scope of the invention to the use of an URL address as a dynamic string.

URL (Uniform Resource Locator) is the address of a file (resource) accessible on the Internet. The type of resource depends on the Internet application protocol. Using the World Wide Web's protocol, the Hypertext Transfer Protocol (HTTP), the resource can be an HTML page, an image file, a program such as a common gateway interface application or Java applet, or any other file supported by HTTP. The URL contains the name of the protocol required to access the resource, a domain name that identifies a specific computer on the Internet, and a hierarchical description of a file location on the computer.

Socket is a method for communication between a client program and a server program in a network. A socket is defined as "the endpoint in a connection." Sockets are created and used with a set of programming requests or "function calls" sometimes called the sockets application programming interface (API). The most common sockets API is the Berkeley UNIX C interface for sockets. Sockets can also be used for communication between processes within the same computer. Sockets may be used with TCP/IP, UDP and RTP, for instance.

SMS (Short Message Service) is a service for sending messages of up to 160 characters (224 characters if using a 5-bit mode) to mobile phones that use Global System for Mobile (GSM) communication. GSM and SMS service is primarily available in Europe. SMS is similar to paging. However, SMS messages do not require the mobile phone to be active and within range and will be held for a number of days until the phone is active and within range. SMS messages are transmitted within the same cell or to anyone with roaming service capability. They can also be sent to digital phones from a Web site equipped with PC Link or from one digital phone to another.

UDP (User Datagram Protocol) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP. The Trivial File Transfer Protocol (TFTP) uses UDP instead of TCP.

SIP is an Internet Engineering Task Force (IETF) standard protocol for initiating an interactive user session that involves multimedia elements such as video, voice, chat, gaming, and virtual reality.

Like HTTP or SMTP, SIP works in the Application layer of the Open Systems Interconnection (OSI) communications model. The Application layer is the level responsible for ensuring that communication is possible. SIP can establish multimedia sessions or Internet telephony calls, and modify or terminate them. The protocol can also invite participants to unicast or multicast sessions that do not necessarily involve the initiator. Because the SIP supports name mapping and redirection services, it makes it possible for users to initiate and receive communications and services from any location, and for networks to identify the users wherever they are.

RTP (Real-Time Transport Protocol) is an Internet protocol standard that specifies a way for programs to manage the real-time transmission of multimedia data over either unicast or multicast network services. Originally specified in Internet Engineering Task Force (IETF), Request for Comments (RFC) 1889. RTP was designed by the IETF's Audio-Video Transport Working Group to support video conferences with multiple, geographically dispersed participants. RTP is commonly used in Internet telephony applications. RTP does not in itself guarantee real-time delivery of multimedia data

(since this is dependent on network characteristics); it does, however, provide the wherewithal to manage the data as it arrives to best effect.

RTP combines its data transport with a control protocol (RTCP), which makes it possible to monitor data delivery for large multicast networks. Monitoring allows the receiver to detect if there is any packet loss and to compensate for any delay jitter. Both protocols work independently of the underlying Transport layer and Network layer protocols. Information in the RTP header tells the receiver how to reconstruct the data and describes how the codec bit streams are packetized. As a rule, RTP runs on top of the User Datagram Protocol (UDP), although it can use other transport protocols. Both the Session Initiation Protocol (SIP) and H.323 use RTP.

MMS: Multimedia Messaging Service (MMS) is a messaging service for the mobile environment standardized by the WAP Forum and 3GPP. To the end-user MMS is very similar to the Short Message Service (SMS): it provides automatic immediate delivery for user-created content from phone to phone. MMS messages are primarily delivered from phone to phone, but also value-added services can be created by developing applications that send/receive MMS messages to/from phones. MMS also supports e-mail addressing, so that messages can be sent directly to an e-mail address. MMS transport is done using WAP transport and any bearer with WAP capabilities can be used. Thus, MMS is bearer independent and MMS is not limited to only GSM or WCDMA. WAP Wireless Session Protocol (WSP) is used for message transport from phone to MMSC and from MMSC to phone. In addition, WAP push features are used to deliver the message from server to receiving phone.

FIG. 1 depicts an overview of one possible system architecture that can make use of the invention. In FIG. 1, there are three local area networks (LAN 1, LAN 2, LAN 3) connected to each other via the Internet. LAN 1 runs a main portal service that can be accessed by users through the Internet or another communications network, such as a mobile telephone network, an internal data network (intranet) or a public switched telephone network. Through the main portal, there can be offered an access to public services that does not require authentication and also such services that are protected by a user name and password, for instance. The services accessible through the main portal can be located at the LAN 1 or at the LAN 2 or 3. The present invention is best utilised in a situation in which a user first authenticates at the main portal (at LAN 1) and then

wants to transfer to another service or page at LAN 2 or 3 that requires authentication and/or authorization. In this situation, LAN 1 can prepare a dynamic URL pointing to LAN 2 or 3 and containing user authentication and/or authorization information. The dynamic URL is then selected by the user and activated, whereupon the user authentication and/or authorization information is transmitted to LAN 2 or 3, thus enabling LAN 2 or 3 to allow access by the user. Now, the user can use services at LAN 2 or LAN3, respectively, without a separate authentication at LAN 2 or LAN3.

FIG. 2 presents an overview of a process according to one embodiment of the invention. In the process of FIG. 2, the following steps are performed:

1. The user selects a WEB or WAP Portal main page located at a first network resource.

2. The WEB or WAP Portal requests authentication.

3. Authentication is performed with the aid of a suitable authentication method, e.g. the user may input a username and password or use a client certificate. Alternatively, the user can be authenticated by means of a mobile network identity, such as a mobile telephone number, or a parameter sent from the mobile telephone or a smart card attached to it.

4. The WEB or WAP Portal checks that the user is included in its user database.

5. If the user is not found in the DB, the WEB or WAP Portal will reject the user and request the authentication once again.

6. If the user is found in the DB, the WEB or WAP Portal will then fetch the set of WEB or WAP services available to the user in question.

7. If no WEB or WAP services will be found related to that specific user in the DB, the WEB or WAP Portal will inform the user and close the application.

8. If, instead, one or more WEB or WAP services are found related to that specific user in the DB, the WEB or WAP Portal will generate a dynamic URL, or a set of dynamic URL:s, by means of which the user can access to these WEB or WAP services.

9. Once the dynamic URL:s are generated, the WEB or WAP Portal will attach them to the links to the WEB or WAP services available to the user and present these links to the user.

10. The user selects a certain WEB or WAP service he wants to use and the link is activated.

11. The application of the WEB or WAP service selected receives the dynamic URL.

12. The application fetches all the parameters included in the dynamic URL it has received.

13. The application verifies the validity of the URL received.

14. If the URL is found valid, the user will have access to the WEB or WAP service.

15. If, instead, the URL is found to be NOT valid, the application will inform the user of the problem and close that WEB or WAP service.

FIG. 3 describes one process of creating a dynamic URL, according to one embodiment of the invention. This embodiment utilizes a hash algorithm, specifically the MD5 hash algorithm, which is, as such, well known in the art. In the process of FIG. 3, the following steps are performed:

Get and concatenate parameters

Parameters, such as the user name, the timestamp, the name of the service pointed to, the userID and the secret key are caught and concatenated together.

HASH the string with MD5 algorithm.

The aforementioned string of parameters is hashed to a message with the MD5 algorithm. Example:

Message = MD5(massimo+311219991030+shoes+1234567890+**********) = 3C9F471D46838A4BC874E53DB48BA9FC

wherein, the user name = Massimo

the timestamp = 311219991030

the name of the service pointed to = shoes

the userID = 1234567890

the secret key is represented by **********

The output of the MD5 hash algorithm is called a message and is represented in this example by the data string 3C9F471D46838A4BC874E53DB48BA9FC.

Generate the URL

The actual URL is generated by including into the URL 1) the http address of the service pointed to, 2) the parameters, which were got and concatenated before, as such, and 3) the hashed message. For example, an URL of this example looks like this:

http://localhost/shoes.asp?username=massimo&timestamp=311219991030&service=shoes&userid=1234567890&message=3C9F471D46838A4BC874E53DB48BA9FC

Attach URL to the WEB/WAP Service link

The generated URL is attached to the WWW or WAP service link.

FIG. 4 describes one process of validating a dynamic URL, according to one embodiment of the invention. In the process of FIG. 4, which is suited to validating a dynamic URL generated by the process of FIG. 3, the following steps are performed:

1. The second network resource receives the URL for authentication. The HTTP URL of this example looks like this:

   http://localhost/shoes.asp?username=massimo&timestamp=311219991030&service=shoes&userid=1234567890&message=3C9F471D46838A4BC874E53DB48BA9FC

2. The application at the second network resource fetches the parameter included in the URL. In this example, the parameters include: the username, the timestamp, the servicename and the userID.

3. The application checks that the timestamp included in the URL is valid.

4. If the timestamp included in the URL is NOT valid, the application will inform the user and close the service.

5. If, instead, the timestamp included in the URL is valid, the application will proceed to checking the validity of the MD5 message included in the URL.

6. To validate the MD5 message, the application creates a second HASH by inputting into a hash algorithm the parameters fetched from the URL and the same shared secret key that was used to create the original message. The hash algorithm used is, of course, the same as in the first network resource that created the dynamic URL. Preferably, the hash algorithm is MD5.

7. After creating the second HASH, the application will compare the original MD5 message included in the URL (first hash) with the new message just created (second hash).

8. If the messages are identical (the first hash corresponds to the second hash), the URL is valid and the user authorized to use that WEB or WAP service.

9. If instead, the messages are NOT identical (the first hash differs from the second hash), the URL is NOT valid and the user will not be authorized to use that WEB or WAP service based on that URL.

FIG. 5 shows an example of the parameters that can be used in the processes of FIG. 3 and FIG. 4. FIG. 5 shows also a one example of a dynamic URL address comprising.

The dynamic URL address of FIG. 5 comprises an address part pointing to a second network resource and a parameter part. In this example, the address part contains an address: "http://localhost/shoes.asp". The parameter part comprises two subparts,

namely an information subpart and a verification subpart. In this example, the information subpart contains a data string:

"username=massimo&timestamp=311219991030&service=shoes&userid=1234567890"

Hence, the information subpart is further divided into sections that name a parameter and give a value to it. In this example, four parameters are used. The parameters of this example are 1) username of the authenticated user, 2) timestamp, 3) name of the target service at the second network resource, and 4) user identification number. The selection of the parameters can be freely made according to the needs of the application. However, using a timestamp as one parameter has an advantageous effect on the security of the authentication. Also the number of parameters may vary; but, for security reasons, it is good to have at least some parameters as they make it more difficult to break the hash.

After the information subpart, there is shown a verification subpart that contains a parameter "message" and its value. The value of the "message" is received from MD5 hash algorithm using the information subpart and a secret key as an input (shown also in FIG.5).

FIG. 6 describes another process of creating a dynamic URL, according to another embodiment of the invention. This embodiment utilizes the Public Key Infrastructure, which is, as such, well known in the art. In the process of FIG. 6, the following steps are performed:

Get and concatenate parameters

The user name, the timestamp, the service name and the serial number of the certificate of the service are caught and concatenated together. There are also other useful parameters which may be used in the process.

Generate the digital signature using the certificate's Private key

The aforesaid string of parameters is signed with the Private key of the service at the first network resource. For example, a signed string may look like this:

Signature=Sign(massimo+311219991030+shoes+12345AA456DF755890)=
2DDE4R545HJHK4J353J45H3J4H543H5H5J

Generate the URL

The actual URL is generated by including to the URL 1) the http address of the service pointed to, 2) the parameters, which were got and concatenated before, as such, and 3) the digitally signed signature. In this example, the URL looks like this:

http://localhost/shoes.asp?username=massimo&timestamp=311219991030&service=shoes&snumber=12345AA456DF755890&signature=2DDE4R545HJHK4J353J45H3J4H543H5H5J

Attach URL to the WEB/WAP Service link

The generated URL is attached to the WWW or WAP service link.

FIG. 7 describes one process of validating a dynamic URL, according to one embodiment of the invention. In the process of FIG. 7, which is suited to validating a dynamic URL generated by the process of FIG. 6, the following steps are performed:

1. The second network resource receives the URL for authentication. The HTTP URL of this example looks like this:

   http://localhost/shoes.asp?username=massimo&timestamp=311219991030&service=shoes&snumber=12345AA456DF755890&signature=2DDE4R545HJHK4J353J45H3J4H543H5H5J

2. The application will fetch the parameter included in the URL: In this example, the parameters include: the username, the timestamp, the servicename and the serial number of certificate used in signing the URL.

3. The application checks that the timestamp included in the URL is valid.

4. If the timestamp included in the URL is NOT valid, the application will inform the user and close the service.

5. If instead the timestamp included in the URL is valid, the application proceeds with checking the validity of the Digital Signature included in the URL.

6. To validate the Digital Signature, the application creates an HASH of the cleartext fetched from the URL.

7. The application generates another HASH using the Public Key of the same certificate that was used to sign the URL over the Digital Signature received.

8. The application compares the two HASH:s generated.

9. If the two HASH:s are identical, the URL is deemed valid and the user authorized to use that WEB or WAP service.

10. If instead the two HASH:s are NOT identical, the URL is NOT valid and the user will not be authorized to use that WEB or WAP service based on that URL.

FIG. 8 shows an example of the parameters that can be used in the processes of FIG. 6 and FIG. 7. FIG. 8 shows also a one example of a dynamic URL address comprising.

The dynamic URL address of FIG. 8 comprises an address part pointing to a second network resource and a parameter part. In this example, the address part contains an address: "http://localhost/shoes.asp". The parameter part comprises two subparts, namely an information subpart and a verification subpart. In this example, the information subpart contains a data string:

"username=massimo&timestamp=311219991030&service=shoes&snumber=12345AA456DF755890"

Hence, the information subpart is further divided into sections that name a parameter and give a value to it. In this example, four parameters are used. The parameters of this example are 1) username of the authenticated user, 2) timestamp, 3) name of the target service at the second network resource, and 4) a serial number of the digital certificate used in signing the URL. The selection of the parameters can be freely made according to the needs of the application. However, using a timestamp as one parameter has an advantageous effect on the security of the authentication. Also the number of

parameters may vary; but, for security reasons, it is good to have at least some parameters as they make it more difficult to break the hash.

After the information subpart, there is shown a verification subpart that contains a parameter "signature" and its value. The value of the "signature" represents the digital signature of the information subpart, signed with the Private key of the certificate referred to in the information subpart (shown also in FIG. 8).

The above description is only to exemplify the invention and is not intended to limit the scope of protection offered by the claims. The claims are also intended to cover the equivalents thereof and not to be construed literally.

Claims:

1. A method for preparing user authentication and/or authorization information at a first network resource for transmission to a second network resource after authenticating and/or authorizing the user accessing the first network resource, the method comprising:

- a step of preparing a dynamic string comprising at least:
  - an address part pointing to the second network resource, and
  - a parameter part comprising information verifying the user authentication and/or authorization.

2. A method according to claim 1, wherein the step of preparing a dynamic string comprises a step of inputting data into a hash algorithm to form a hash.

3. A method according to claim 1 or 2, wherein the parameter part of the dynamic string comprises an information subpart and a verification subpart.

4. A method according to claim 3, wherein the step of preparing a dynamic string comprises:

- a step of inputting data into a hash algorithm to form a hash, wherein said data includes at least part of the information subpart and a security code unknown to a third party, and
- using the thus formed hash as the verification subpart.

5. A method according to claim 3, wherein the step of preparing a dynamic string comprises:

- a step of inputting data into a hash algorithm to form a hash, wherein said data includes at least part of the information subpart, and
- digitally signing the thus formed hash to form a digital signature, and
- using the thus formed digital signature as the verification subpart.

6. A method according to claim 5, wherein the information subpart includes data relating to the digital signature, such as the serial number of the certificate used in

producing the digital signature, which data is included in the data input into the hash algorithm.

7. A method according to any of claims 4 to 6, wherein the information subpart includes a data indicating a point of time and wherein said data indicating a point of time is included in the data that is input into a hash algorithm.

8. A method according to claim 7, wherein said data indicating a point of time is a time stamp given for the user authentication and/or authorization at the first network resource.

9. A method according to any of claims 1 to 8, wherein the information subpart of the dynamic string includes the user name and/or the user ID of the authenticated and/or authorized user.

10. A method according to any of claims 1 to 9, wherein the information subpart of the dynamic string includes parameters relating to a service at the second network

11. A method according to claim 2, wherein the data inputted into the hash algorithm includes a secret key of the first network resource and the step of preparing a dynamic string comprises

- a step of placing said hash into the parameter part of the dynamic string.

12. A method according to claim 2, wherein the first network resource has a private key of an asymmetric cryptographic method and the step of preparing a dynamic string further comprises:

- a step of inputting said hash and the private key into the asymmetric cryptographic algorithm to form a digital signature, and
- a step of placing the digital signature into the parameter part of the dynamic string.

13. A method according to claim 1, wherein the step of preparing a dynamic string comprises:

- obtaining a time stamp for the user authentication and/or authorization,

- preparing an address part pointing to the second network resource,
- preparing an information parameter part including the time stamp and parameters relating to a service at the second network resource and/or the user,
- obtaining a secret key shared by the first and second network resources,
- inputting the address part, the information parameter part and the secret key into a hash algorithm to form a hash, and
- attaching the address part, the information parameter part and the hash to form the dynamic string.

14. A method according to claim 1, wherein the step of preparing a dynamic string comprises:

- obtaining a time stamp for the user authentication and/or authorization,
- preparing an address part pointing to the second network resource,
- preparing an information parameter part including the time stamp, the serial number of the digital certificate of the first network resource, and parameters relating to a service at the second network resource and/or the user,
- inputting the address part and the information parameter part into a hash algorithm to form a hash,
- signing the hash with the digital signature relating to the digital certificate, whose serial number is included in the information parameter part, to form a digital signature, and
- attaching the address part, the information parameter part and the digital signature to form the dynamic string.

15. A method for accepting, at a second network resource, a user authentication and/or authorization performed at a first network resource, the method comprising:

- receiving, as a parameter in a dynamic string prepared by the first network resource and directed to the second network resource, information on the user authentication and/or authorization performed at the first network resource,
- using a cryptographic method to verify the received user authentication and/or authorization information, and after verification
- accepting the user as an authenticated and/or authorized user at the second network resource.

16. A method according to claim 15, wherein the received information on the user authentication and/or authorization includes a hash, and wherein the step of using a cryptographic method to verify the received user authentication and/or authorization information comprises:

- a step of inputting data into a hash algorithm to form a hash,
- comparing the formed hash with the received hash, and
- accepting the user authentication and/or authorization as verified only if the formed hash and the received hash are identical.

17. A method according to claim 15, wherein the received dynamic string includes an information subpart and a hash, and wherein the step of using a cryptographic method to verify the received user authentication and/or authorization information comprises:

- inputting data into a hash algorithm to form a hash, wherein said data includes at least part of the information subpart and a security code unknown to a third party,
- comparing the formed hash with the received hash, and
- accepting the user authentication and/or authorization as verified only if the formed hash and the received hash are identical.

18. A method according to claim 15, wherein the received information on the user authentication and/or authorization includes a digital signature, and wherein the step of using a cryptographic method to verify the received user authentication and/or authorization information comprises verifying the digital signature.

19. A method according to claim 18, wherein the received dynamic string includes data relating to the digital signature, such as the serial number of the certificate used in producing the digital signature, and the step of using a cryptographic method to verify the received user authentication and/or authorization information further comprises:

- a step of checking the validity of the certificate and/or the identity of the signing party with the aid of the data relating to the digital signature.

20. A method according to any of claims 15 to 19, wherein the received dynamic string includes data indicating a point of time, and further comprising:

- checking the point of time against a security criterion, and
- denying the user authentication and/or authorization if the security criterion is not met.

21. A method according to any of claims 15 to 19, wherein the received dynamic string includes a time stamp given for the user authentication and/or authorization at the first network resource, and further comprising:

- a step of checking the validity of the time stamp, and
- a step of denying the user authentication and/or authorization if the time stamp has expired.

22. A method according to any of claims 15 to 20, wherein the received dynamic string includes the user name and/or the user ID of the authenticated and/or authorized user.

23. A method according to any of claims 15 to 21, wherein the received dynamic string includes parameters relating to a service at the second network.

24. A method according to claim 15, wherein the step of using a cryptographic method to verify the received user authentication and/or authorization information involves using a secret key shared with the first network resource.

25. A method according to claim 15, wherein the step of using a cryptographic method to verify the received user authentication and/or authorization information comprises the steps of:

- obtaining a first hash from the dynamic string,
- obtaining an information parameter part of the dynamic string, said information parameter part including
  - the time stamp for the user authentication and/or authorization, and
  - parameters relating to a service at the second network resource and/or the user,
- obtaining a secret key shared by the first and second network resources,
- inputting the information parameter part and the secret key into a hash algorithm to form a second hash,
- checking the first hash against the second hash, and
- denying the user authentication and/or authorization if the first hash differs from the second hash.

26. A method according to claim 15, wherein the step of using a cryptographic method to verify the received user authentication and/or authorization information comprises the steps of:

- obtaining a digital signature from the dynamic string,
- obtaining an information parameter part of the dynamic string, said information parameter part including a time stamp for the user authentication and/or authorization and the serial number of the digital certificate used in producing the digital signature,
- obtaining the public key of the digital certificate used in producing the digital signature,
- checking the time stamp,

- checking the validity of the obtained digital signature with the aid of said information parameter part and said public key, and
- denying the user authentication and/or authorization if the digital signature is not valid or if the time stamp has expired.

27. A method according to claim 26, further comprising the steps of:

- checking the validity of the digital certificate with the aid of the serial number of the digital certificate, and
- denying the user authentication and/or authorization if the digital certificate is not valid or if the time stamp has expired.

28. A method according to any of claims 15 to 27, wherein the user is accepted as an authenticated and/or authorized user at the second network resource exclusively on the basis of the received dynamic string, without using any user database external to the second network server.

29. A method according to any of claims 15 to 28, wherein the dynamic string is a dynamic URL address.

30. A method according to claim 29, further comprising the steps of:

- obtaining, from the HTTP Server, the IP address of the network resource that has sent the dynamic URL address,
- checking whether the obtained IP address appears on a list of acceptable IP addresses, and
- denying the user authentication and/or authorization if the obtained IP address does not appear on the list of acceptable IP addresses.

31. A method according to any of claims 15 to 30, wherein the accepted user authentication and/or authorization relates to the first network resource, or an entity within the first network resource, and authenticates and/or authorizes said resource or entity for operations performed with the second network resource.

32. A method according to any of claims 15 to 30, wherein the accepted user authentication and/or authorization relates to an entity external to the first network resource, and authenticates and/or authorizes said entity for operations performed with the second network resource.

33. A method of forwarding user authentication and/or authorization from a first network resource to a second network resource, the method comprising:

- a step of transmitting information verifying the user authentication and/or authorization from a first network resource to a second network resource as a part of a dynamic string pointing to the second network resource.

34. A method according to claim 33, wherein the information verifying the user authentication and/or authorization includes a digital signature.

35. A method according to claim 33 or 34, wherein the information verifying the user authentication and/or authorization includes a time stamp given to the user authentication and/or authorization at the first network resource.

36. A method according to any of claims 33 to 35, wherein the information verifying the user authentication and/or authorization includes a secret code known to the first and second network resource but unobtainable to a third party.

37. A method according to any of claims 33 to 36, wherein the user authentication and/or authorization information relates to an entity within the first network resource.

38. A method according to any of claims 33 to 36, wherein the forwarded user authentication and/or authorization authorizes the first network resource to use services or resources of the second network resource, or perform operations at the second network resource.

39. A method according to any of claims 33 to 36, wherein the user authentication and/or authorization information relates to an entity external to the first network resource but first authenticated and/or authorized with the first network resource.

40. A computer program product configured to transmit information to a second network resource, said computer program product comprising:

- computer readable program code means for preparing user authentication and/or authorization information,
- computer readable program code means for preparing a dynamic string comprising said user authentication and/or authorization information, and
- computer readable program code means for directing said dynamic string to the second network resource.

41. A computer program product configured to receive information from a first network resource, said computer program product comprising:

- computer readable program code means for receiving a dynamic string from the first network resource,
- computer readable program code means for extracting user authentication and/or authorization information from said dynamic string,
- computer readable program code means for verifying said user authentication and/or authorization information, and
- computer readable program code means configured to authenticate the user or grant authorization to the user if said user authentication and/or authorization information is deemed verified.

FIG. 1

LAN 1
WEB/WAP Main Portal
Service Digital Certificate or
secret key
INTERNET
LAN 2
WEB/WAP Service
Shared Digital Certificate or
secret key
LAN 3
WEB/WAP Service
Shared Digital Certificate or
secret key

FIG. 2

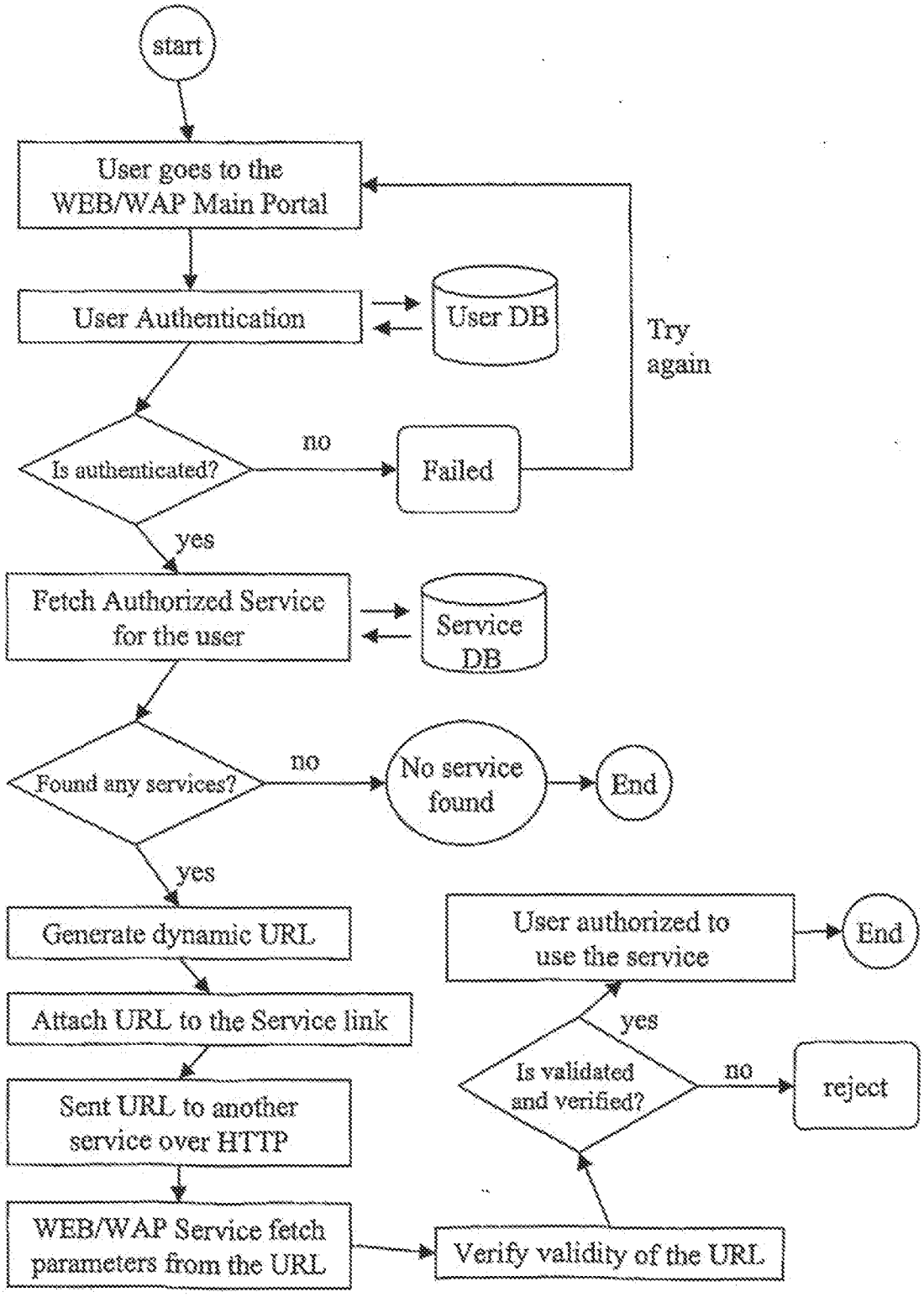

start
User goes to the WEB/WAP Main Portal
User Authentication
User DB
Try again
Is authenticated?
no
Failed
yes
Fetch Authorized Service for the user
Service DB
Found any services?
no
No service found
End
yes
Generate dynamic URL
Attach URL to the Service link
Sent URL to another service over HTTP
WEB/WAP Service fetch parameters from the URL
Verify validity of the URL
Is validated and verified?
yes
no
reject
User authorized to use the service
End

FIG. 3

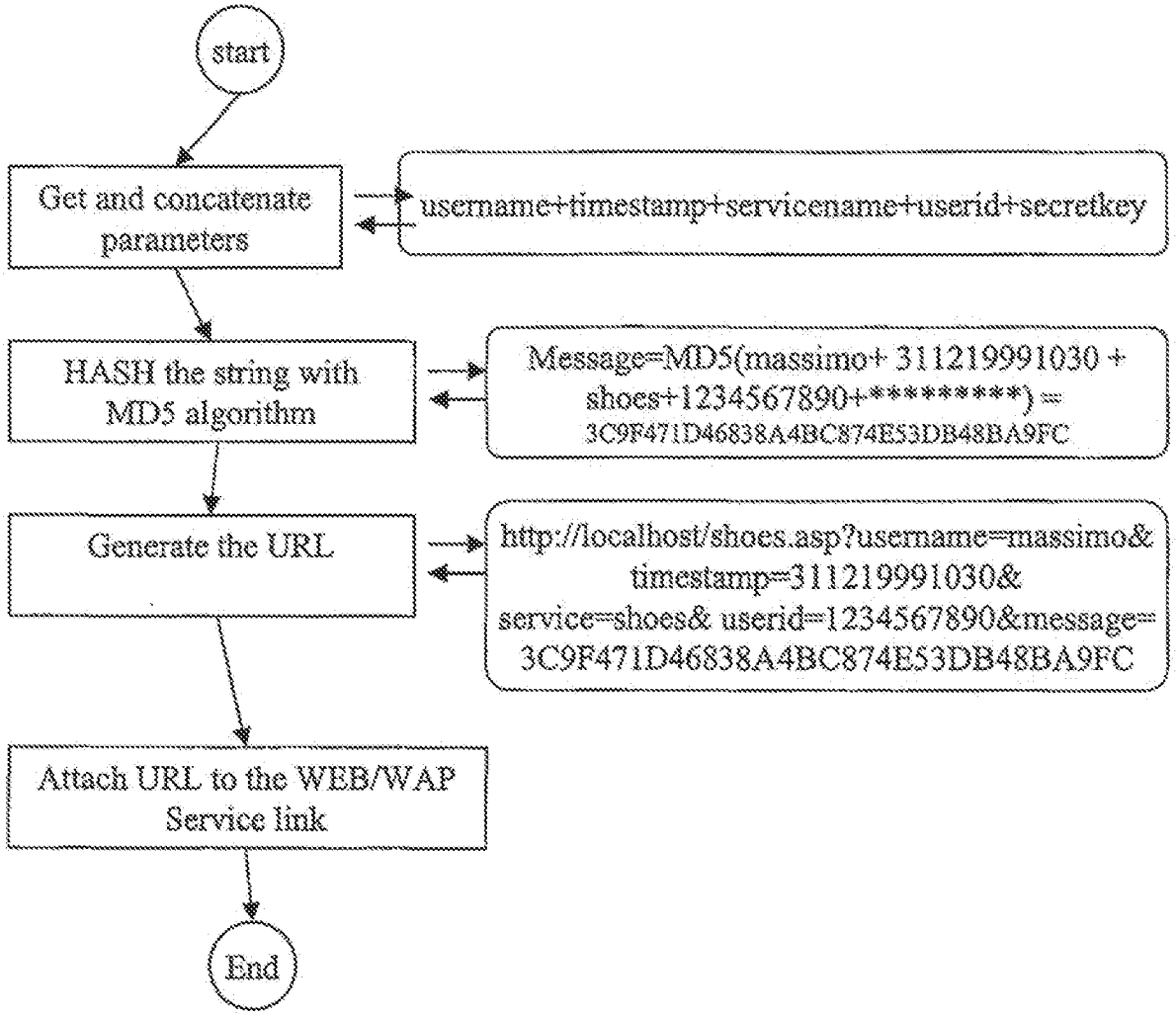

start
Get and concatenate parameters
username+timestamp+servicename+userid+secretkey
HASH the string with MD5 algorithm
Message=MD5(massimo+ 311219991030 + shoes+1234567890+*********) = 3C9F471D46838A4BC874E53DB48BA9FC
Generate the URL
http://localhost/shoes.asp?username=massimo& timestamp=311219991030& service=shoes& userid=1234567890&message= 3C9F471D46838A4BC874E53DB48BA9FC
Attach URL to the WEB/WAP Service link
End

FIG. 4

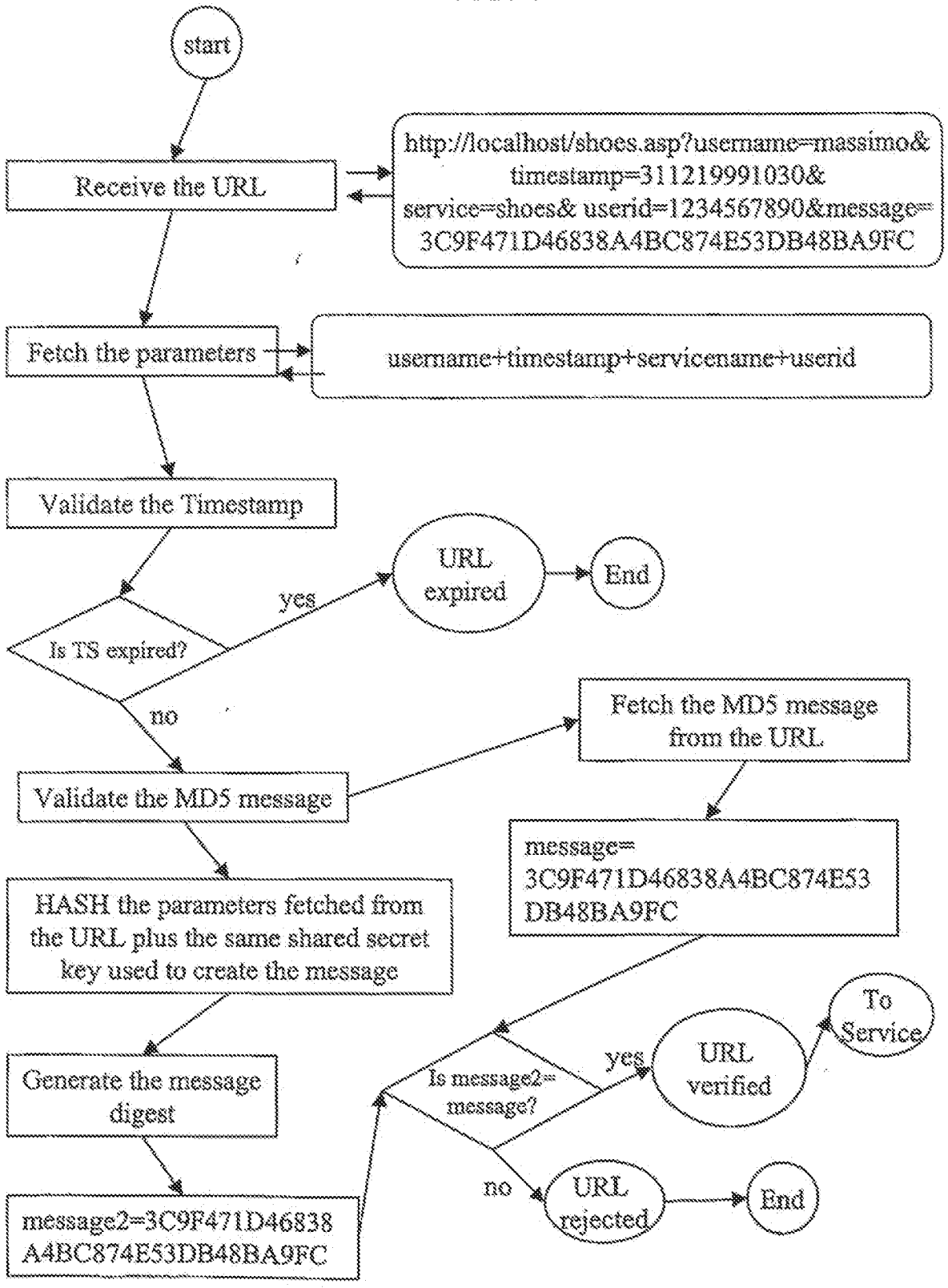

start
Receive the URL
http://localhost/shoes.asp?username=massimo&
timestamp=311219991030&
service=shoes& userid=1234567890&message=
3C9F471D46838A4BC874E53DB48BA9FC
Fetch the parameters
username+timestamp+servicename+userid
Validate the Timestamp
Is TS expired?
yes
URL expired
End
no
Validate the MD5 message
Fetch the MD5 message from the URL
message=
3C9F471D46838A4BC874E53
DB48BA9FC
HASH the parameters fetched from the URL plus the same shared secret key used to create the message
Generate the message digest
message2=3C9F471D46838
A4BC874E53DB48BA9FC
Is message2= message?
yes
URL verified
To Service
no
URL rejected
End

FIG. 5

USERNAME	TIMESTAMP	SERVICENAME	USERID	SECRETKEY
massimo	311219991030	shoes	1234567890	**********

Message =MD5(username+timestamp+servicename+userid+secretkey)

Message=MD5(massimo+ 311219991030 +shoes+1234567890+**********) = 3C9F471D46838A4BC874E53DB48BA9FC

http://localhost/shoes.asp?username=massimo&timestamp= 311219991030&
service=shoes&userid=1234567890&message=3C9F471D46838A4BC874E53DB48BA9FC

FIG. 6

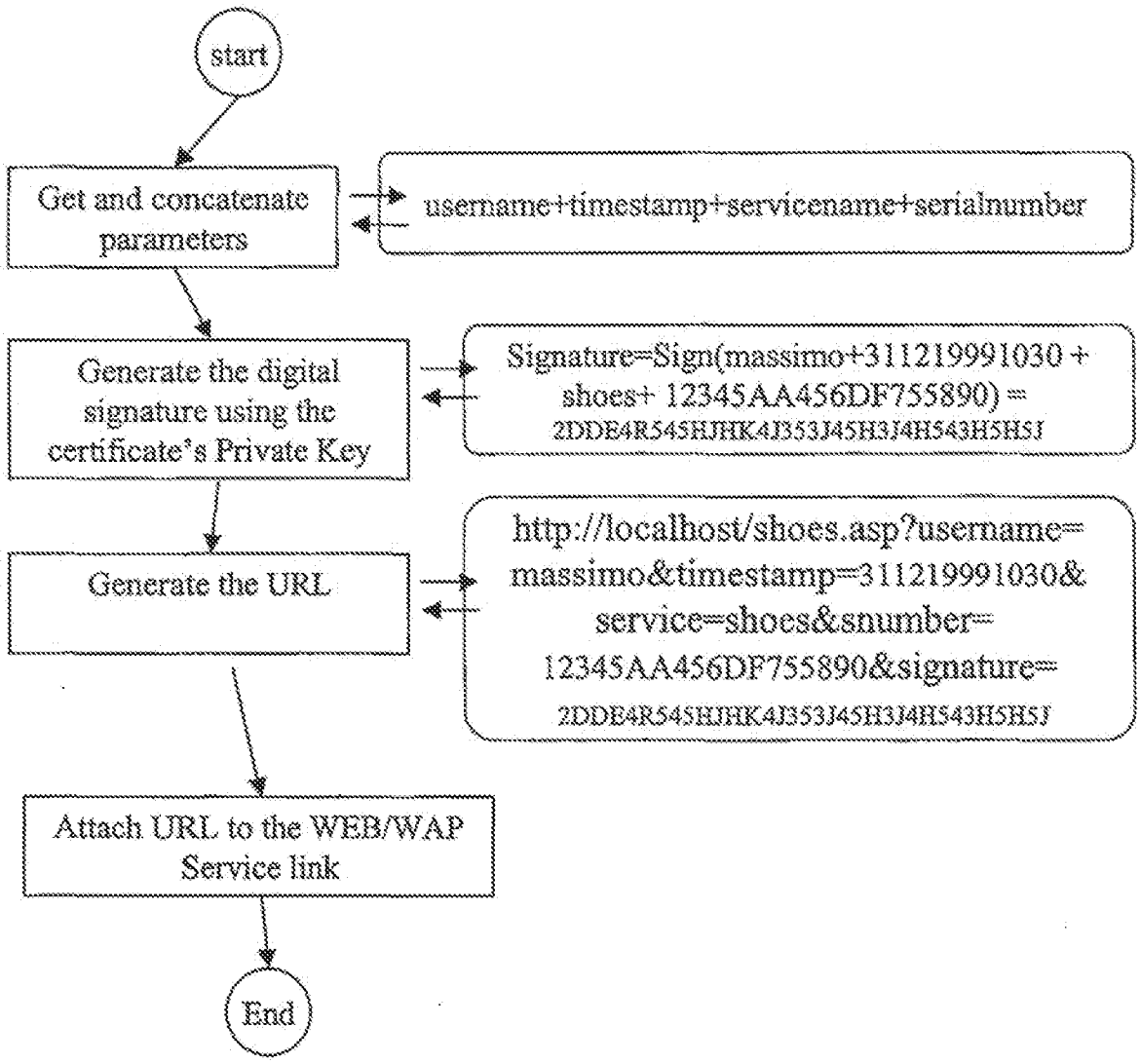

start
Get and concatenate parameters
username+timestamp+servicename+serialnumber
Generate the digital signature using the certificate's Private Key
Signature=Sign(massimo+311219991030 + shoes+ 12345AA456DF755890) = 2DDE4R545HJHK4J353J45H3J4H543H5H5J
Generate the URL
http://localhost/shoes.asp?username= massimo&timestamp=311219991030& service=shoes&snumber= 12345AA456DF755890&signature= 2DDE4R545HJHK4J353J45H3J4H543H5H5J
Attach URL to the WEB/WAP Service link
End

FIG. 7

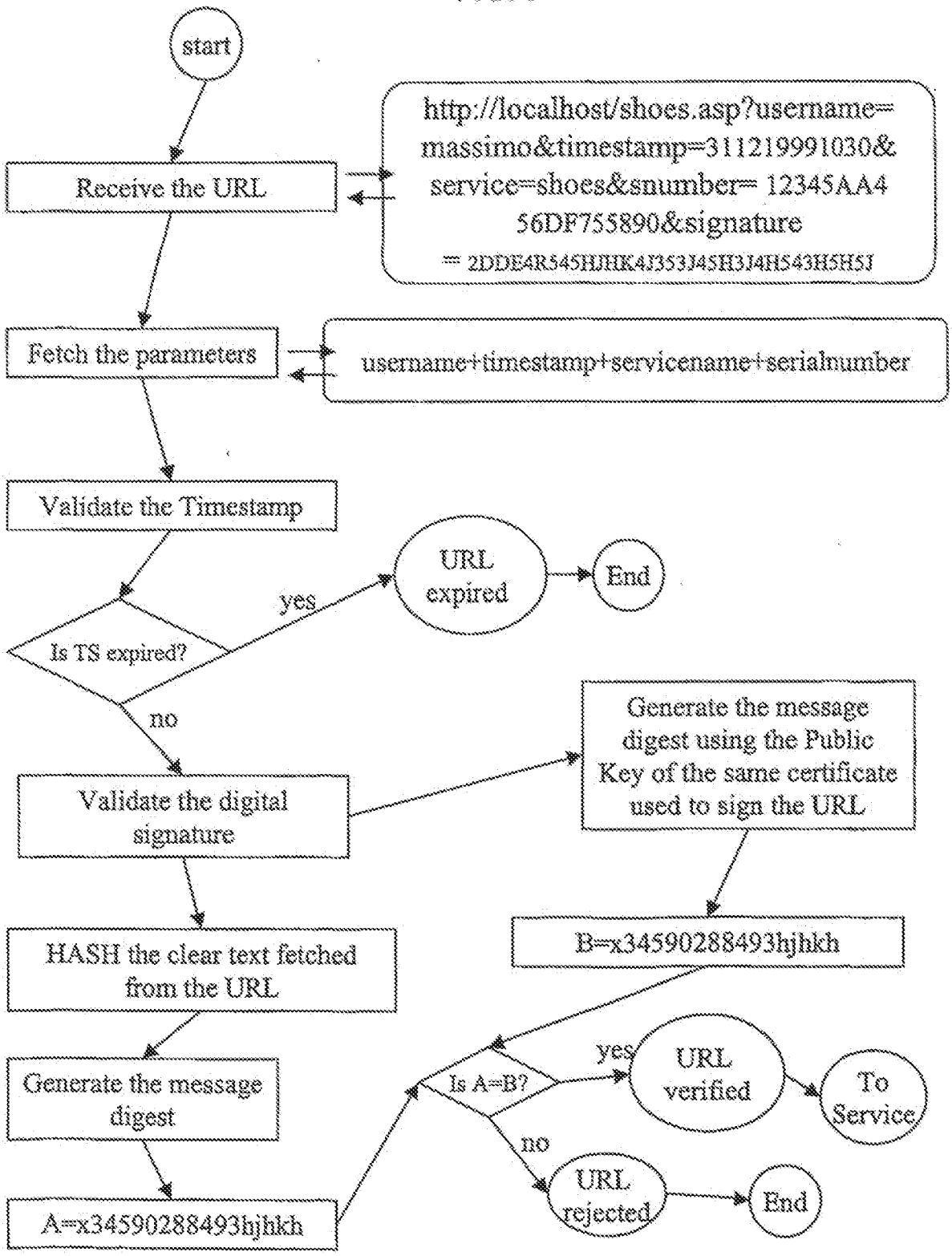

start
Receive the URL
http://localhost/shoes.asp?username=massimo&timestamp=311219991030&service=shoes&snumber= 12345AA456DF755890&signature = 2DDE4R545HJHK4J353J45H3J4H543H5H5J
Fetch the parameters
username+timestamp+servicename+serialnumber
Validate the Timestamp
Is TS expired?
yes
URL expired
End
no
Validate the digital signature
Generate the message digest using the Public Key of the same certificate used to sign the URL
HASH the clear text fetched from the URL
B=x34590288493hjhkh
Generate the message digest
A=x34590288493hjhkh
Is A=B?
yes
URL verified
To Service
no
URL rejected
End

FIG. 8

USERNAME	TIMESTAMP	SERVICENAME	CERTIFICATE SERIALNUMBER
massimo	311219991030	shoes	12345AA456DF755890

Signature=Sign(username+timestamp+servicename+serialnumber)

Signature=Sign(massimo+311219991030 +shoes+ 12345AA456DF755890) = 2DDE4R545HJHK4J353J45H3J4H543H5H5J

http://localhost/shoes.asp?username=massimo&timestamp=311219991030&
service=shoes&snumber= 12345AA456DF755890&signature= 2DDE4R545HJHK4J353J45H3J4H543H5H5J

WO 03/077522A2
PCT/IB02/00572

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 02/00572

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 1/00, H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL WPI DATA

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5812776 A (GIFFORD, D.K.), 22 Sept 1998 (22.09.98), column 4, line 20 - column 5, line 43	1-41
A	US 6189096 B1 (HAVERTY, R.), 13 February 2001 (13.02.01), figure 9, abstract	6,14,19,26, 27

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 November 2002	03 -12- 2002
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Jenny Forss/LR Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

28/10/02

International application No.
PCT/FI 02/00572

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5812776 A	22/09/98	AU 694367 B	16/07/98
		AU 5936796 A	09/01/97
		CA 2221506 A	27/12/96
		EP 0830774 A	25/03/98
		JP 11507752 T	06/07/99
		JP 2002157180 A	31/05/02
		WO 9642041 A	27/12/96
US 6189096 B1	13/02/01	AU 3624599 A	23/11/99
		CA 2330958 A	11/11/99
		CN 1299545 T	13/06/01
		EP 1076953 A	21/02/01
		JP 2002514842 T	21/05/02
		WO 9957846 A	11/11/99